IN THE SPECIFICATION

Please replace paragraph [0007] at pages 5-6, with the following rewritten paragraph:

[0007] In order to execute a key exchange protocol in IPSec, communication is performed multiple times between apparatuses which mutually agree on SA information. Furthermore, a lot of computation processing amount is required by the communication, which imposes a considerable load on the apparatuses. If, to cope with this, an SA information agreement function is provided for a small-sized terminal in a home, such as electronic equipment provided with a cryptographic-processed communication function, the scale of hardware and software is increased, and the size and the price are also increased. From this point of view, it is proposed, for example, in Japanese Patent Application Laid Open No. 2003-179592 (hereinafter referred to as Patent Literature 2) that, though a terminal is provided with a cryptographic processing function, processing of agreeing on SA information is substituted by a key ~~support~~ exchange proxy apparatus on behalf of the terminal. According to the key exchange substitution technique shown in this Patent Literature 2, when a terminal which is connected to a network and which is provided with a cryptographic processing function but is not provided with a key exchange function, performs packet cryptographic communication with a communication counterpart terminal which is connected to the network and provided with a key exchange function, the terminal [[32]] first requests exchange of common keys to be used for a cryptographic communication signal with the communication counterpart terminal, from a key exchange proxy server connected to the network, and the key exchange proxy server performs key exchange processing with the communication counterpart terminal on behalf of the terminal based on the request and sets an agreed common key for the terminal. After that, the terminal uses the agreed common key to perform packet cryptographic communication with the communication counterpart terminal.

Please replace paragraph [0012] at page 8, with the following rewritten paragraph:

[0012] As described above, according to the packet cryptographic processing proxy apparatus of this invention, since it is connected between a network and a terminal, a counterpart apparatus connected to the Internet, for example, can perform cryptographic processing, for example, decryption of a packet for which cryptographic processing has been performed, only by setting the IP address or the like of a terminal which is not provided with a cryptographic processing function. That is, the counterpart apparatus can employ a transport mode, and the user of the counterpart apparatus is not required to make settings such as the IP address of the terminal and the IP address of the packet cryptographic processing proxy apparatus and does not have to make such troublesome settings. It is also not necessary to do troublesome works of obtaining the IP address or the like of the cryptographic processing proxy server via communication with the terminal, and, after that, setting the IP address of the server to send a packet for which cryptographic processing has been performed to the cryptographic processing proxy server.

Please replace the paragraph at page 20, line 24 to page 21, line 8, with the following rewritten paragraph:

Fig. 4 is a flowchart of a process to be performed for a packet received by the packet cryptographic processing proxy apparatus 10 from a terminal 5. Similarly to the case of Fig. 3, when a packet is received at step S11, it is determined whether or not the packet requests agreement on cryptographic communication channel information (SA information) (for example, exchange of cryptographic keys (step S12). If the packets requests it, the cryptographic communication channel information is agreed with the counterpart apparatus 3 at step [[S3]] S13, and the agreed cryptographic communication channel information is written in the cryptographic communication channel information storage 12 in association with a terminal IP address. The process then returns to step S11 and receives the next packet.

Please replace paragraph [0039] at page 25, with the following rewritten paragraph:

[0039] Fig. 7 is a flowchart showing a process for agreeing on cryptographic communication channel information to be performed for a packet received from a terminal 5, by the packet cryptographic processing proxy apparatus. Steps S12-1 to S12-4 in Fig. 7 show details of step S12 in Fig. 3, and steps S13-1 to S13-4 in Fig. 7 show details of step S13 in Fig. [[3]] 4. The process of Fig. 7 is almost the same as that of Fig. 6.